What is claimed is:

1. A method for reducing the vulnerability of an enterprise network to a malicious code attack from a virtual private network (VPN) capable end system, comprising:

denying network access to a VPN capable end system before a user on the end system becomes authenticated;

permitting network access by the end system solely on at least one VPN connection to an enterprise network once the user on the end system becomes authenticated; and

permitting write access to the end system solely to at least one temporary memory while the VPN connection is active.

2. The method of claim 1, wherein the recited steps are performed on the end system.

3. The method of claim 1, further comprising the step of purging the temporary memory once the VPN connection becomes inactive.

4. The method of claim 1, further comprising the step of authenticating the user.

5. The method of claim 4, wherein the authenticating step comprises a two factor user authentication.

6. The method of claim 1, wherein the step of permitting network access comprises dropping packets that are not associated with the VPN connection.

7. The method of claim 1, wherein the step of permitting write access comprises directing data writes to a RAM disk on the end system.

8. The method of claim 1, further comprising the step of logging the user off the end system once the VPN connection becomes inactive.

9. The method of claim 1, further comprising the step of restarting the end system once the VPN connection becomes inactive.

10. The method of claim 1, further comprising the step of shutting down the end system once the VPN connection becomes inactive.

11. The method of claim 1, wherein the VPN connection becomes inactive through an action initiated on the end system.

12. The method of claim 1, wherein the VPN connection becomes inactive through an action initiated external to the end system.

13. A virtual private network (VPN) capable end system, comprising:

at least one permanent memory;

at least one temporary memory;

at least one processor coupled to the permanent memory and the temporary memory; and

operating software stored on the permanent memory, the operating software having instructions executable by the processor to deny network access to the end system before a user on the end system becomes authenticated and, once the user on the end system becomes authenticated, to permit network access by the end system solely on at least one VPN connection to an enterprise network and permit write access solely to the temporary memory while the VPN connection is active.

14. The end system of claim 13, wherein the operating software has instructions executable by the processor to purge the temporary memory once the VPN connection becomes inactive.

15. The end system of claim 13, wherein the operating software has instructions executable by the processor to authenticate the user.

16. The end system of claim 13, wherein the operating software has instructions executable by the processor to drop packets that are not associated with the VPN connection.

17. The end system of claim 13, wherein the operating software has instructions executable by the processor to log the user off the end system once the VPN connection becomes inactive.

18. The end system of claim 13, wherein the operating software has instructions executable by the processor to restart the end system once the VPN connection becomes inactive.

19. The end system of claim 13, wherein the operating software has instructions executable by the processor to shut down the end system once the VPN connection becomes inactive.

20. The end system of claim 13, wherein the permanent memory is a nonvolatile memory.

21. The end system of claim 13, wherein the temporary memory is a RAM disk.

22. Operating software for a virtual private network (VPN) capable end system comprising instructions executable by at least one processor on the end system to deny network access to the end system before a user on the end system becomes authenticated and, once the user on the end system becomes authenticated, to permit network access by the end system solely on at least one VPN connection to an enterprise network and permit write access solely to at least one temporary memory on the end system while the VPN connection is active.

23. The software of claim 22, further comprising instructions executable by the processor to purge the temporary memory once the VPN connection becomes inactive.

24. The software of claim 22, further comprising instructions executable by the processor to authenticate the user.

25. The software of claim 22, further comprising instructions executable by the processor to drop packets that are not associated with the VPN connection.

26. The software of claim 22, further comprising instructions executable by the processor to log the user off the end system once the VPN connection becomes inactive.

27. The software of claim 22, further comprising instructions executable by the processor to restart the end system once the VPN connection becomes inactive.

28. The software of claim 22, further comprising instructions executable by the processor to shut down the end system once the VPN connection becomes inactive.